



TITLE:

ShibbolethによるOffice365 Educationのシングルサインオン

AUTHOR(S):

上田, 浩

CITATION:

上田, 浩. ShibbolethによるOffice365 Educationのシングルサインオン.
2013

ISSUE DATE:

2013-12-06

URL:

<http://hdl.handle.net/2433/179557>

RIGHT:

Shibboleth による Office365 Education のシングルサインオン

京都大学 学術情報メディアセンター 上田 浩*

概要

京都大学では 2013 年 8 月 19 日から 20 日で、学生用メールシステムの Live@edu から Office365 への移行を、8 月 26 日に Office365 の Shibboleth 認証連携を完了した。本稿では、移行内容の概要と Shibboleth 連携を実現するためのシステム開発、Office365 の評価、今後の展望と課題を述べる。

1 はじめに

インターネットをはじめとする情報通信サービスは大学における実験的サービスから発展してきた。その中でも大学が学生、教職員に提供するメールサービスは、各種サービスの中でも比較的初期から存在し、利用者にとっても、運用側にとっても一定のプライオリティが存在してきた。現在ではメールサービスが教育研究活動を支える重要なインフラストラクチャになっていると言っても過言ではなく、教務系システムや LMS などとメールサービスの連携による各種通知はごく当たり前に行われている。

このような背景のもと、管理運用コストの削減、情報システムの集約による最適化、ICT の進歩への対応などのコンテキストから、学内にメールシステムを全て整備するのではなく、Google Apps for Education, Office365 Education (以下、Office365 と表記する) などの学外のクラウド型サービスへ移行し、大学のメールシステムを物理的、論理的に大学のネットワークの外部で運用する事例が報告されている [1, 2, 3]。

京都大学 (以下本学と表記する) では 2011 年 12 月よりマイクロソフトのクラウドメールサービス (Live@edu with Outlook Live, 以下 Live@edu と表記する) を採用した、学生用メールサービスを開始した [4, 5]^{*1}。サービス開始時点から、マイクロソ

フト社のクラウドメールサービスは Office365 に移行することが予定されており^{*2}、本学では 2013 年 8 月 19 日から 20 日で Live@edu から Office365 への移行を、8 月 26 日に Office365 と本学統合認証基盤との Shibboleth 認証連携を完了した。

本稿では、まず 2 節で学生用メールサービスの概要を述べ、次いで 3 節で Live@edu から Office365 への移行のインパクト、4 節で Office365 への移行と Shibboleth 認証連携を実現するためのシステム開発、5 節で管理運用と移行プロジェクトについて説明し、6 節で現時点での Office365 の評価、今後の展望と課題を述べる。

2 学生用メールサービス KUMOI の概要

学生用メールサービス KUMOI^{*3}について、要件、システム構成、利用状況の概要を述べる。

2.1 要件:認証連携, 多様性への対応, 頑健性

本学には学生向けアカウント ECS-ID と、教職員向けのアカウントである SPS-ID の 2 つの ID 体系が存在する。KUMOI の利用者は ECS-ID 利用者である。ECS-ID は教育用コンピュータシステムの利用コードをその前身として持ち、全学生に入学時に配布している。

ECS-ID は学内の様々なサービスの認証に用いる

* @UEDA.Hiroshi, uep@media.kyoto-u.ac.jp

*1 一方、教職員向けのメールサービスは学内システムによる提供となっている。

*2 Office365 は 2011 年の時点ではシングルサインオンができないなどの機能不足があり、SSO Toolkit が利用できる Live@edu を採用せざるを得なかった。

*3 愛称「雲居」Kyoto University Mail clOud Interface, 公募による選定。

ため、これまで本学では ECS-ID とメールアドレスには明示的な関連がない形で運用してきた。このポリシーを継続できることに加え、ストーキングや迷惑メール対策などのためメールアドレスを変更できることが望ましく、認証連携が必須である。

また、ECS-ID は SPS-ID を利用できない本学構成員の受け皿となっているという歴史的経緯があり、利用者には一部の教職員、名誉教授、非常勤講師なども含まれる。これら合計 25,000 人以上の多様な利用者に対応できるものでなければならない^{*4}。

メールサービスは教育研究活動に加え、研究発表や就職活動など対外的活動、長期休暇時の連絡手段として利用されることが予想されるため、メンテナンスのため長期間サービスを停止することが事実上困難であるため、サービスが停止することがない、頑健なシステムであることが求められる。

これらの要件を満たすサービスを低コストで実現することを目指し、本学はクラウドメールサービスによる外部委託を選択した*5。

2.2 KUMOI のシステム構成

Office365 移行前後の KUMOI の仕様を表 1 に示す。メールアドレスが氏名をもとにしたものとなっているため、関係する各部局と協議を重ね、氏名などの学籍情報からメールアドレスを生成するワークフローを整備した。Office365 移行前後の大きな違いは認証基盤と認証連携の方式となり、詳細には 3 節の通りである。

KUMOI のバックエンドは、企業で多数導入実績がある、Exchange Server 2010 であり Office365 でも共通である。1 アカウントあたり 10G のメールボックス容量を提供でき、スマートフォンからのアクセスも可能である。メールを読み書きする Web UI は Outlook Web App (以下 OWA と表記する、図 1) と呼ばれ、デスクトップアプリケーションに

表 1 KUMOI の仕様

	Live@edu	Office365(Web14)
メールアドレス	kyodai.hanako.xxx@st.kyoto-u.ac.jp	
ID	Windows Live	Microsoft Online Services
認証連携	SSO Toolkit	Shibboleth, ADFS
ライセンス	無償	有料プランあり
メールサーバー	Exchange Online (Exchange Server 2010 相当)	
メールボックス容量	10G/アカウント	
ファイル共有	SkyDrive	SharePoint Online
メッセージング	Windows Messenger	Lync Online
組織ロゴの追加	可能	不可能
SLA	なし	有料プランのみ 99.9%

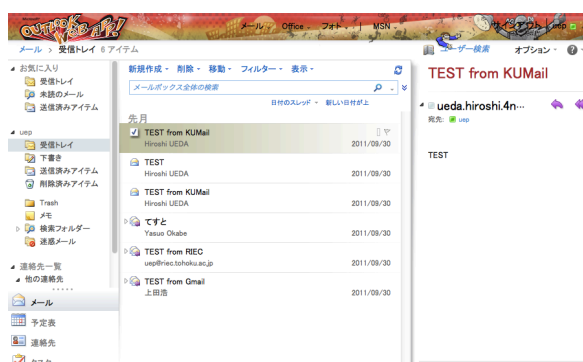


図1 Outlook Web App スクリーンショット

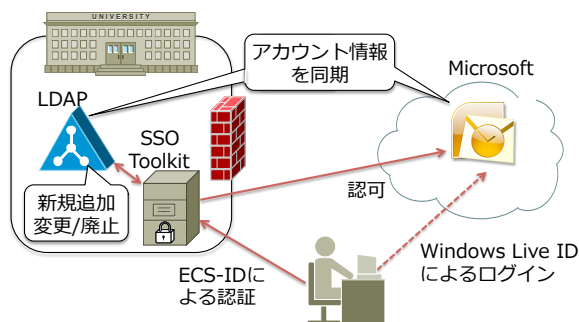


図2 Office365 移行前の KUMOI のシステム構成

準じたデザインとなっているため、Outlook ユーザであれば違和感なく利用できると思われる。

2.2.1 Office365 移行前

Office365 移行前のシステム構成を図 2 に示す。Live@edu はユーザ ID として Windows Live ID すなわちメールアドレスを用いるため、ECS-ID による認証連携を次の通り行っていた (図 2)。

- 本学統合認証システムの LDAP サーバーと Live@edu に登録されるアカウント情報を

*4 このような事情があり、メールを送受信するサブドメインとして“st.kyoto-u.ac.jp”を選択した。

*5 クラウド型メールサービスにはマイクロソフトの他に Google, Yahoo! のサービスがあるが、本学では法的問題を相対的にクリアしていることに加え、学内認証基盤との連携のため同社サービスを採用した。詳しくは [4] を参照されたい。

PowerShell で同期

- Live@edu SSO ToolKit を導入し ECS-ID による認証と Live@edu 間でシングルサインオン

この構成では学内は ECS-ID、クラウドでは Windows Live ID での認証となっていた*6。

2.2.2 Office365 移行後

クラウドサービスにおけるシステム移行はサービスへの影響は無いのが一般的であるが、Live@edu から Office365 への移行は認証基盤の移行を意味し、学内認証基盤との認証連携を行っている場合、学内システムに大きなインパクトがあることが判明した。加えて、以前からの課題であった本学統合認証基盤との Shibboleth 連携を実現するため、本移行に合わせ、関連するシステムをほぼ再構築することとなった。詳しくは 4 節で述べる。

2.3 利用状況

マイクロソフトのクラウドサービスを採用した KUMOI は、サービスを開始した 2011 年 12 月から現在まで、2.4 節で述べる名前解決の障害をはじめとする深刻なものが見られることを除けば、大規模な障害は発生しておらず、サービスを継続することができた。図 3 に KUMOI の「到達率」を 2012 年 4 月から 2013 年 8 月までを示す。本稿執筆時点では、7 割ていどの学生が KUMOI を利用していることになる。到達率は次の式で定義されるアカウント数の比であり、長期休暇期間は OWA へのログイン数が低くなっていることが分かる。

$$\text{到達率} = \frac{\text{該当月に OWA にログイン} \cap \text{転送設定済み}}{\text{有効な ECS-ID}}$$

2013 年度の夏季休暇時の到達率の減少が 2012 年度のそれよりも少ないのは、KUMOI から携帯電話のメールなどへの転送設定を行っている利用者が多くなったことが原因であると考えられる (図 4)。

2.4 システム障害と不具合の改善

自組織でメールシステムを構築、サービス提供を行っている場合と違い、クラウドメールサービスのように、システムがブラックボックスになっている

*6 Live@edu によるサービス開始当初はクラウドでの認証のみ。2012 年 3 月 21 日から認証連携を開始した。

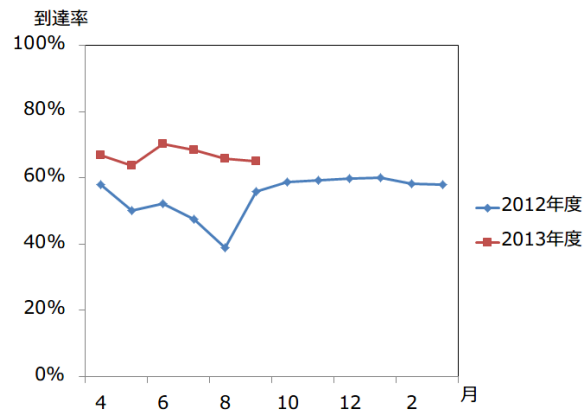


図 3 KUMOI 到達率

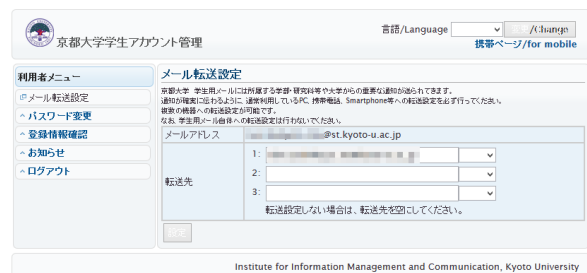


図 4 転送設定 Web UI

場合には、迅速な対応が困難な場合がある。これまでの障害と不具合のうち大きなものを挙げる。

メールボックスが突然無くなったように見える

OWA にログインするため認証すると、“This account does not have an Outlook Web App Mailbox.” と表示され (図 5), OWA にアクセスできないという障害が 2012 年 9 月 25 日に発生した。原因はデータセンター内ネットワーク装置が停止したこととの報告を受けている。

名前解決の障害で学内から KUMOI 向けメールが遅延

KUMOI, すなわち st.kyoto-u.ac.jp ドメインの MX はマイクロソフトのデータセンター側に設定されている。2012 年 11 月 9 日、2013 年 1 月 29 日、学内メールシステムから st.kyoto-u.ac.jp へのメールを送信する際の MX の名前解決に失敗した。2 度も同じ障害が発生したこと自体有り得ないことであるが、事

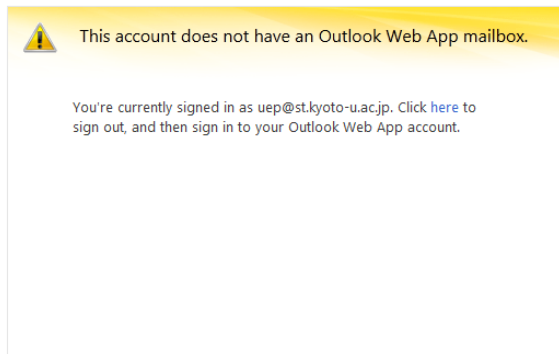


図 5 “This account does not have an Outlook Web App Mailbox.” と表示されメールボックスが無くなったように見える

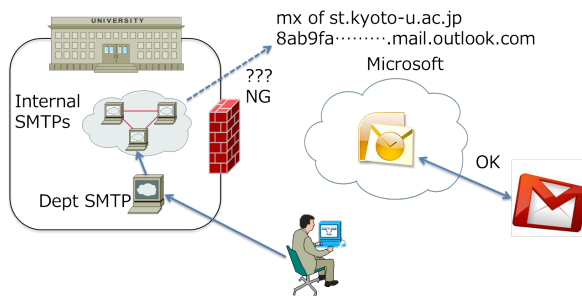


図 6 学内からの MX の問い合わせに失敗する

象は同じであっても原因は異なっていた。11月の障害はデータセンター内のスイッチ設定不足 (DNS ANY, AAAA クエリがブロックされていた)、1月はマイクロソフトの DNS システム更新時の不具合 (詳細は不明。「“Not implemented” という予期せぬ問題 (報告書原文のまま)」とのこと)。

日本語のメールが GB2312 で送信され本文が読めない OWA でテキスト形式のメールを外部へ送信した場合にごくまれに GB2312 と判定されるといふ Exchange Server の既知の不具合であり、動作設定の変更で回避するようにとマイクロソフトからの指示があった。本不具合については他大学からの報告もなされている [6]。

“We need you to add some security info ...”

Live@edu の認証基盤は Windows Live である。2012 年 6 月上旬に行われた Windows

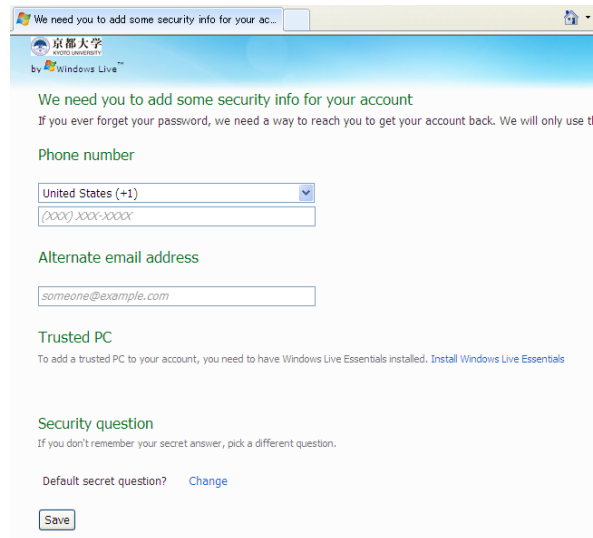


図 7 “We need you to add some security info ...”

Live のセキュリティ強化は Live@edu にも影響があり、OWA にログインすると追加のセキュリティ情報を入力するよう、パスワードは学内ポリシーに合わせているにもかかわらず「標準的なセキュリティ要件^{*7}に合わないパスワードの変更」が求められるようになり (図 7)、当惑したユーザへの対応に苦慮した (本変更は 8 月 9 日にロールバックされた^{*8})。

3 Live@edu から Office365 への移行のインパクト

Live@edu と Office365 の違いを表 1 に示す。Office365 とはその名の通りメールシステムだけではなく、Office アプリケーションと情報共有のためのポータルサイト、オンライン会議、ファイル共有などのクラウドサービスを一体化した課金型のサービスであり、最も大きな違いは認証基盤とライセンスの考え方である。利用にあたり、本学では無償のプラン A2 を利用するため月額コストは不要である^{*9}。

^{*7} 非公開

^{*8} 7 月 18 日時点では「ロールバックは行わない」との回答であったにもかかわらずである。

^{*9} その他 Office アプリケーションが利用できるプラン A3、さらにエンタープライズボイス機能 (自動応答) が加わるプラン A4 がある。Office365 の利

今回の移行において最もインパクトが大きいのが認証基盤の変更であり、ユーザ ID が Windows Live ID から Microsoft Online Services ID に変更されることにより、学内統合認証システムと Windows Live ID を同期する手順と認証連携を行う SSO Toolkit が動作しなくなることが分かった。また、これまでの Windows Live ID は削除されず残ることから、移行の際ユーザへの周知をどのように行うかについても課題があることが分かった。

認証基盤の変更は運用側にとっては大きな問題である。加えて、Office365 はサブスクリプションベースの製品のため、Live@edu から移行した場合にもユーザー一人一人に対し新規ライセンスの付与が必要となる。加えて、Office365 ではライセンスの付与は管理者が Web UI で行うことが想定されており、大学のように一時に多くの新規ユーザを一括登録し、同時にライセンス付与を行う仕組みが存在しない。

Office365 ではマイクロソフトのクラウドメールシステムとしては初めて Shibboleth 連携がサポートされた。本学は様々な Web システムの Shibboleth 連携を進めており、KUMOI についてもシングルサインオンが実現できる環境が整った。

4 移行と Shibboleth 連携のためのシステム開発

Live@edu から Office365 への移行はマイクロソフトのデータセンター側で自動的に行われるため、移行そのものに対するシステム開発は不要である。移行は次の 2 つの観点で捉えることができる。

認証基盤 Live@edu のログインアカウント（つまりメールアドレス）と Exchange Online プラン 1 のライセンス情報が Windows Live ID から Microsoft Online Services ID へ移行される
メールボックス Live@edu の Exchange Online テナントから Office365 の Exchange Online へ

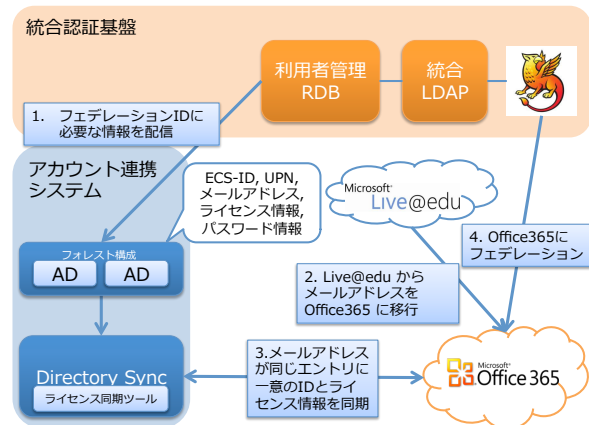


図 8 アカウント連携システムによる Office365 への移行概要

移行される^{*10}

マイクロソフトのデータセンター側で行われる移行が完了した段階では、Microsoft Online Services ID での認証が可能となっているだけで、学内 ID によるシングルサインオンはできない。

Office365 にはクラウド ID(Microsoft Online Services ID のこと Office365 で認証を行う) とフェデレーション ID の 2 通りの ID があるとされており、シングルサインオンを行うためにはフェデレーション ID の構成を取る必要がある。このためには、学内に Active Directory を持っており、Office365 側の Active Directory と定期的に同期を取ることが前提である。本学では Active Directory を Windows 端末の認証には利用しているものの ID 管理には利用していないため、統合認証基盤のサーバー群からフェデレーション ID の配信を受け管理する Active Directory などからなる Office365 向けアカウント連携システム（以後アカウント連携システム）を新規導入した（図 8）。

4.1 アカウント連携システムによる Office365 への移行

Office365 向けアカウント連携システムは Active Directory（2 台によるフォレスト構成）とディレク

点は SLA (Service Level Agreement) であるが、無料プランについては SLA ありの記載がなく我々は混乱した。 <http://office.microsoft.com/ja-jp/academic/FX103045755.aspx>

^{*10} これについては確認がないが、Live@edu と Office 365 の OWA は少しの見た目の変化があった。

トリ/ライセンス同期サーバから構成される。本システムによりフェデレーション ID への移行が次のように行われる。

1. 本学統合認証基盤からアカウント連携システムの Active Directory に、連携に必要とされる属性を含む ID 情報を配信する
2. マイクロソフト データセンター側で Office365 への移行を行う
3. アカウント連携システムの Active Directory 内のアカウントの ObjectGUID を、Microsoft Online Services ID 内のメールアドレスが一致するアカウントの ImmutableID に登録し紐付け、同時にアカウントに Office365 プラン A2 のライセンスを割り当てる
4. KUMOI で受信するドメイン (st.kyoto-u.ac.jp) を Shibboleth フェデレーションするドメインに設定する

新規ユーザ登録、メールアドレスの変更が行われる際、統合認証基盤の利用者管理システムからの配信を受けディレクトリ同期を行うという流れは同じである。ディレクトリ同期ツールの仕様上、3 時間に一度の同期となっている。加えて、Office365 を利用するためにはライセンスの付与が行わなければならないが、前述の通り、ディレクトリ同期と同時にライセンス付与が行われない (Directory Sync の仕様上の制限) ため、ライセンス同期ツールを新規開発した。ライセンス同期ツールは深夜に一日一度動作させる運用となっている^{*11}。

4.2 Shibboleth 認証連携による Office365 へのシングルサインオン

アカウント連携システムにより利用者が Office365 の Web システムにシングルサインオンすることができる (図 9)。

1. 利用者が Web ブラウザで Shibboleth IdP のフォーム認証ページで ECS-ID とパスワードを送信し認証リクエストを行う

^{*11} 新規ユーザはユーザ登録後 KUMOI の利用まで実質的には一日待つ必要があり、改善の余地はある。

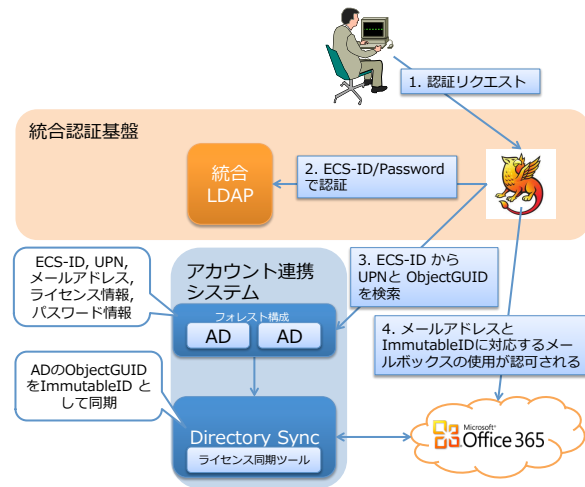


図 9 Shibboleth 認証連携による Office365 へのシングルサインオン

2. Shibboleth IdP が統合 LDAP サーバを参照し、ECS-ID とパスワードによる認証を行う
3. Shibboleth IdP が ECS-ID を検索し、UPN^{*12} (初期メールアドレス) と ObjectGUID^{*13} を取得し Office365 へ送信
4. UPN と ObjectID の値を Office365 のユーザ名、ImmutableID として検索し、対応するメールボックスへのアクセスが認可される

4.3 Shibboleth 認証連携による Exchange Online への IMAP/SMTP 接続

IMAP/SMTP による Exchange Online の利用はシングルサインオンではなくシングルパスワードとなるものの、以下の通り可能である (図 10)。より詳しい技術情報は [7] を参照されたい^{*14}。

1. IMAP/SMTP クライアントがユーザ名「ECS-ID@st.kyoto-u.ac.jp」として Exchange Online ({imap,pop,smtp}.office365.com) に接続
2. Exchange Online は st.kyoto-u.ac.jp をフェデ

^{*12} userPrincipalName

^{*13} Active Directory がすべてのオブジェクトに対して付している一意な ID (128bit のランダムな数値)。

^{*14} より詳細には、同 Web ページの「次に、現在のメタデータの値を示します」以降のボックス内のデータを Office365 の Metadata として Shibboleth IdP に登録する必要があった。

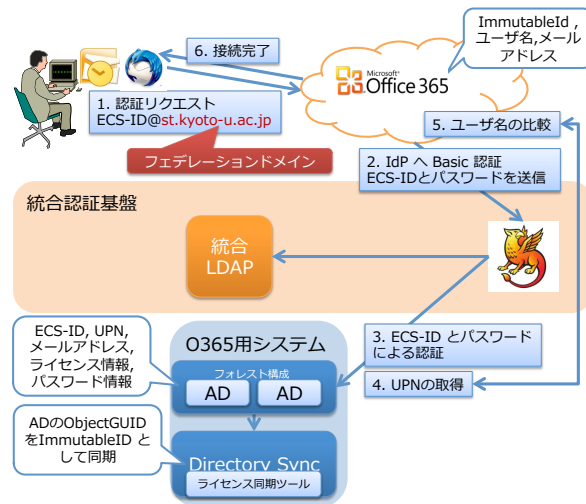


図 10 Shibboleth 認証連携による Exchange Online への IMAP/SMTP 接続

レーションドメインと認識し、@の左側つまり ECS-ID を Shibboleth IdP に送信し Basic 認証のリクエストを行う

3. Shibboleth IdP がアカウント連携システムの Active Directory で ECS-ID とパスワードによる認証を行う
4. 認証に成功したユーザの UPN を取得
5. 取得した UPN をキーに Office365 のユーザ名を検索
6. 検索結果のユーザ名に対応するメールボックスへの IMAP/SMTP アクセスが認可される

5 移行プロジェクト

2012 年夏から Shibboleth 連携による Office365 の運用を実現するためのシステムの検討を進め、2012 年 10 月に Active Directory と Directory Sync を核とする構成が承認された。我々は 2013 年夏を Office365 への移行日と定め、2013 年 1 月に移行プロジェクトをスタートした。

5.1 システム構築とリハーサル

アカウント連携システムの構築は 2013 年 3 月末に完了した。2013 年 4 月から運用を含めたシステムテストを行い、6 月、7 月に実運用されていない Live@edu のテナントを 2 つ利用し移行リハーサル

を行った。Live@edu から Office365 への移行自体は多数の事例があり、マイクロソフトのデータセンタで完結するものであるが、フェデレーション ID の構成、かつ Shibboleth IdP との連携を行った移行事例は我々の知る限り存在しなかったことから、移行には慎重にならざるを得なかった。この対応のため、前述のリハーサル用テナント 2 つの確保に加え、アカウント連携システムを学内の VM (仮想マシン) ホスティングサービスを利用し構築した。VM ホスティングサービスには物理サーバーの管理が不要であることのほか、移行リハーサルの際に VM のスナップショットを取ることでリハーサル前の環境に戻すことができるため、リハーサル用のサーバを別途確保する必要がないという利点があるからである。

1 回目のリハーサルは 6/17 に開始した。残念ながらリハーサル用に確保した Live@edu テナントが登録可能なアカウント数が 10,000 に制限されており、データ移行そのものに関する検証はできたものの、KUMOI 利用者のすべてのアカウントが移行するための時間を予測することはできなかった。

2 回目のリハーサルは 7/5 に開始し、35,000 ユーザーで約 29 時間を要した。これで、移行には 48 時間を要すると想定することとした。これはマイクロソフトのデータセンター内でのアップグレードにかかる時間であり、フェデレーション ID の構成のための作業は含まれていない。

5.2 KUMOI の Office365 への移行

リハーサルの結果を踏まえ、KUMOI の Office365 への移行を 8/19 に開始した。4.1 節の通りに進めることとなるが、詳細には次の通りである。

1. 本学統合認証基盤の利用者管理システムの停止 (8/19 9:00 ~)。フェデレーション ID を構成するためのディレクトリ同期を行う準備のためである。停止している間、新規アカウントの登録や削除、ユーザー自身のパスワードの変更などのアカウント情報の変更が行えない。
2. 利用者管理システムからアカウント連携システムへのアカウント情報配信 (8/19 16:00 ~)。

3. マイクロソフトデータセンターでの Live@edu から Office365 への移行 (8/20 15:00 ~). Live@edu 管理ポータル (edusadmin.live.com) で「アップグレード」ボタンをクリックすることで開始される。アップグレードは同日 20:49 に完了したこと、6 時間で完了したことになる。

4. アップグレード完了後、管理者ポータルは portal.microsoftonline.com と変更される。また、管理者 ID のドメインはフェデレーションドメインである「st.kyoto-u.ac.jp」を簡略化した「stkyotouac.onmicrosoft.com」となる。これはフェデレーションドメインの ID ではクラウド側での認証ができないことを回避するためと思われる。またこの時点ではフェデレーションが完了しておらずクラウド ID での認証となるためユーザーはメールアドレスとパスワードログイン認証となる (図 11)。移行の際少なくとも 3 名のユーザのパスワード移行に失敗していることが判明したため、管理者側でクラウド ID のパスワードリセットを行った。

5. Directry Sync の有効化と同期、ライセンス付与 (8/21 00:00 ~ 8/23 5:00)

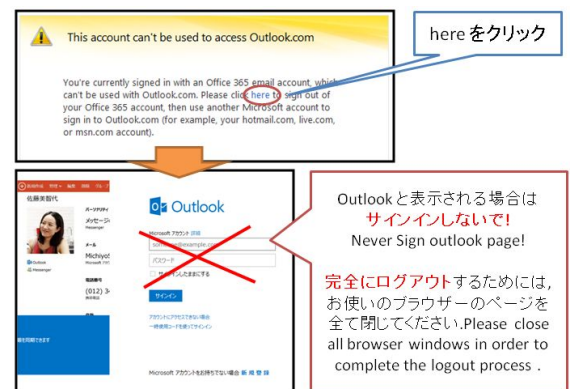
6. Shibboleth フェデレーションを有効化 (8/26 9:30 ~)。有効化直後の時間帯はアカウントによっては Shibboleth 認証になったりならなかったりと不安定な挙動を繰り返し、安定するまで数時間必要であった。また、フェデレーションが有効になると、IMAP/SMTP クライアントが送信すべきユーザ名は ECS-ID@st.kyoto-u.ac.jp となることについてユーザへのアナウンスを行った。

6 本事例の評価、今後の展望と課題

移行期間の 1 週間、メール送受信のサービス自体は停止することなく継続できたことから、本移行はひとまず成功であると考えられる。ユーザーにとっての使い勝手に変化はほとんどないが、Office365 を Shibboleth 認証連携で運用することにより、認

	状態	アクセスするURL	注意点
8/19(月) 16:00	システム更新前	http://mail.st.kyoto-u.ac.jp	・通常の KUMOI のログイン画面が表示されます ・ECS-ID とパスワードでログインしてください
	システム更新中	http://mail.st.kyoto-u.ac.jp	・通常の KUMOI のログイン画面が表示されます ・ECS-ID とパスワードでログインしてください ・ログインできない場合はもう1つのURLからログインして下さい
8/26(月) 12:00	システム更新中	http://mail.office365.com/	・Office365 と表示されたログイン画面が表示されます ・メールアドレスとパスワードでログインしてください ・ログインできない場合はもう1つのURLからログインして下さい
	システム更新後	http://mail.st.kyoto-u.ac.jp	・「学習」と表示されたログイン画面が表示されます ・ECS-ID とパスワードでログインしてください

図 11 移行期間中の Outlook Web App へのアクセス方法 (<http://www.iimc.kyoto-u.ac.jp/ja/services/mail/kumoi/mvo365.html> より)



学生用メールの <http://mail.st.kyoto-u.ac.jp> からアクセスすると、認証画面が表示されます。学生の方は全学生共通ポータル<https://student.iimc.kyoto-u.ac.jp/> からご利用いただけます。



図 12 “This account can't be...” 問題を解決する手順 (<http://www.iimc.kyoto-u.ac.jp/ja/services/mail/kumoi/mvo365.html> より)

証の統合を進めることができた。しかしながら、本移行自体は率直に言うとマイクロソフトの都合で認証基盤のみの移行が行なわれたと言っても過言ではなく、現時点では Office365 (バージョン Web14 と呼ばれている) へのアップグレードによる改善点を見つけられない。むしろ Live@edu から“ダウングレード”となっている次の点が見受けられる。

ブランド連携の廃止 OWA の左上隅に大学のロゴ



図 13 Office365 のライセンス上の構成



図 14 KUMOI ロゴ.

など任意の画像を入れることができない。本学では KUMOI デザインプロジェクトを立ち上げブランド連携を意図したロゴ (図 14) を制定したがその成果を反映できない。また、OWA に大学独自の Web リンク (Live@edu による運用時には学務系システムや LMS などへのリンクを作成していた) を作成することができない。Office Web Apps の実質的廃止 マイクロソフトのクラウドサービスを利用する利点の一つに、ブラウザによる Office 文書の編集が挙げられる。Live@edu や Outlook.com には添付ファイルを「ブラウザで編集」というボタンがあり、Office アプリケーションを持ってなくても編集できるが、Office365 では閲覧のみである^{*15}。すなわち、マイクロソフトのクラウドサービスを利用する意義が無い状態である。

^{*15} SharePoint にアップロードすればブラウザで編集できる。

一方、移行により Shibboleth 連携が実現したことは評価できる。Live@edu での運用時は、IMAP/SMTP での利用状況が全く不明であった^{*16}が、Shibboleth 連携による IMAP/SMTP 利用となったことから、認証のログを取得できるようになり、より正確な利用状況の把握が可能となった。

移行により予想しなかったユーザー対応が必要となった場合があった。多くのユーザーは KUMOI を Web メールとして利用しており、我々も OWA でのメール送受信を推奨している。Office365 移行前に OWA の URL (<https://podXXXX.outlook.com/owa/> などとなる) をブラウザのブックマーク機能で保存し、Office365 移行後にブックマークに記録された URL にアクセスすると、Office365 とテナントが違うため図 12 上のようなエラーが表示されユーザは困惑する。加えて困ったことに「click here」と表示されているリンクをクリックすると Windows Live ID でログインすべき Outlook.com にリダイレクトされてしまう。これを回避するには、Live ID からログアウトした後 (フェデレーションが有効な) 正規のログイン Web ページからのアクセスを行えば良いが、一般ユーザにこの挙動と理由を理解してもらうのは困難であった。

移行後も引き続き、マイクロソフトのデータセンター側不具合が報告されている。9/17,18 に、利用者より KUMOI の言語設定がユーザーの意図しない言語に切り替わり、一旦他の言語になってしまうと日本語に戻せないという不具合が発生した [8]。また、Live@edu 時からの問題として、Exchange Online が扱えない文字コードのメールを受信できないだけでなく、エラーメッセージすら出さない仕様であることが確認されており、我々はマイクロソフトに不具合改善を継続的に要望している [9]。

Office365 の Exchange Online 以外のサービスをどのように利用するかという運用上の課題がある (図 13)。本学では、オンライン会議アプリケーションである Lync Online は Shibboleth フェデレー

^{*16} Exchange Online にログを蓄積する機能が実質的にないことに加え、クラウド認証となるため。

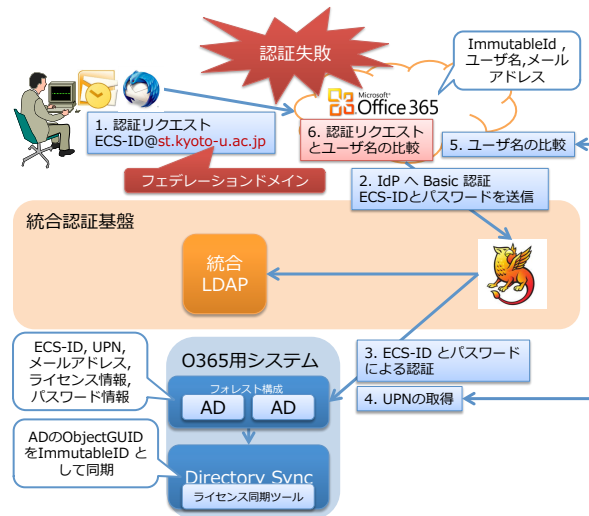


図15 Web15におけるIMAP/SMTP認証の流れ。「6. 認証リクエストとユーザ名の比較」で両者が一致しなければフェデレーション失敗となる。

ションに対応していないため、また、SharePointは共有Webポータルを構築できるサービスであるが、学内の他サービスとの重複が予想されるため提供しないこととした。

Office365はWeb15と呼ばれるバージョンにサービスアップグレードすることが予定されている^{*17}。しかしながら、Office365への移行直後の2013年9月に、Web15ではIMAP/SMTPクライアントとの認証シーケンスが変更され、本学のフェデレーションID構成ではIMAP/SMTP認証に失敗するバグがあることが判明した(図15)。本バグはサービスの根幹にかかわるものであるため、本学テナントについてはサービスアップグレードを延期し、バグ修正をマイクロソフトに要望している。

7 おわりに

メールシステムに限らず、情報システムのクラウド化が世の中のトレンドであるかのように進められているが、本学のクラウド-クラウド移行事例は、クラウド化の功罪とそのオンプレミスにはないリス

クを示すものである。我々は“トレンド”や“パスワード”に惑わされるのではなく、今一度、情報システムそのものの品質と運用について真摯に考え直すべき時に立っているのではないだろうか。

謝辞

本事業の実現にあたり多大なるご指導をいただいた、京都大学情報環境機構関係各位、アカウント連携システムの構築をご担当いただいたサイオステクノロジー株式会社、また技術的支援をいただいた日本電気株式会社、日本マイクロソフト株式会社各位に厚く御礼申し上げます。

参考文献

- [1] 稗田, 河野, 岡山, 山井, 大隅, 中島, 深見, 久保田: “Google Appsによる岡山大学全学メールサービスの実現”, 学術情報処理研究, 13, pp. 111-115 (2009).
- [2] 下園: “生涯メールサービスについて”, 鹿児島大学情報基盤センター「年報」, pp. 8-27 (2009).
- [3] 上田: “群馬大学におけるGoogle Apps/Gmailの導入と運用”, 東京農工大学, 国立情報学研究所共催シンポジウム「キャンパス情報基盤の運営における課題と展望: 学術クラウドサービス時代に向けて」, 東京農工大学 小金井キャンパス, pp. 3-18 (2009).
- [4] 上田, 上原, 植木, 外村, 石井, 森, 古村, 針木, 岡部: “京都大学におけるクラウドメールサービスの運用”, 大学ICT推進協議会2011年度年次大会論文集, 福岡国際会議場, pp. 371-373 (2011).
- [5] 上田: “京都大学におけるクラウドメールサービスの運用”, クラウドサービスのためのSINET及び学認説明会, キャンパスプラザ京都 (2011).
- [6] 藤村: “福岡大学におけるクラウドサービス導入の考え方”, CTCアカデミックユーザーアソシエーション会誌 ViewPoint, No. 12, pp. 39-41 (2012).
- [7] Microsoft: “シングルサインオンで使用するShibbolethを構成する” (2013).
- [8] 京都大学情報環境機構: “【KUMOI】学生用メール(KUMOI)の言語設定が変更されてしまう” (2013).
- [9] 京都大学情報環境機構: “【全学メールシステム】学生用メールへのメール不到達について” (2013).

^{*17} Live@edu から Office365 への移行の場合、まず Web14 に移行した後でなければ Web15 へのサービスアップグレードは不可能である。